IN THE CLAIMS

Upon entry of the present amendment, the status of the claims will be as is shown below. The present listing of claims replaces all previous versions and listings of claims in the present application.

Claims 1-7 (Cancelled)

8. (New) A method of exchanging digital data over a communications link between a first party having a unique first digital data and a second party having a unique second digital data, the method comprising:

the first party encrypting the first digital data and generating an authentication certificate, the authentication certificate authenticating that the encrypted first digital data is an encryption of the first digital data, and sending the encrypted first digital data and the authentication certificate to the second party;

the second party verifying that the encrypted first digital data is an encryption of the first digital data using the authentication certificate, and the second party sending the second digital data to the first party when the encrypted first digital data is an encryption of the first digital data;

the first party verifying that the second digital data is valid and, when the second digital data is valid, the first party accepting the second digital data and sending the unencrypted first digital data to the second party;

the second party verifying that the unencrypted first digital data is valid and, when the unencrypted first digital data is valid, the second party accepting the unencrypted first digital data and, when the unencrypted first digital data is invalid, the second party sending the encrypted first digital data and the second digital data to a third party, the third party having a decryption key to decrypt the encrypted first digital data; and

the third party receiving the encrypted first digital data and the second digital data from the second party when the unencrypted first digital data is invalid, the third party decrypting the encrypted first digital data to obtain the decrypted first digital data, verifying that the decrypted first and the second digital data are valid and, when the decrypted first and the second digital data are valid, sending the decrypted first digital data to the second party and the second digital data to the first party.

9. (New) The method according to claim 8, in which the first and second digital data are on files M_A and M_B respectively, the first party encrypting the first digital data on a concatenation of file M_A and a one-way hash of file M_B; and, when the encrypted first digital data is an encryption of the first digital data, the second party encrypting the second digital data on a concatenation of file M_B and a one-way hash of file M_A.

10. (New) The method according to claim 8, wherein the first and second digital data are digital signatures belonging to the first and second party, respectively.

11. (New) The method according to claim 8, wherein the second digital data is a secret file M which the first party wishes to receive from the second party in exchange for the first digital data.

12. (New) The method according to claim 8, wherein the first party has a pair of public/private keys in a first digital signature scheme; the second party has a pair of public/private keys in a second digital signature scheme; and the third party has a pair of public/private keys in a public key encryption scheme.

13. (New) The method according to claim 12, wherein the digital signature schemes are discrete logarithm based schemes; and the public key encryption scheme is a discrete logarithm based scheme.

14. (New) The method according to claim 12, wherein the digital signature schemes are Guillou-Quisquater type digital signature schemes; and the public key encryption scheme is a discrete logarithm based scheme.

15. (New) The method according to claim 9, wherein the first and second digital data are digital signatures belonging to the first and second party, respectively.

16. (New) The method according to claim 9, wherein the first party has a pair of public/private keys in a first digital signature scheme; the second party has a pair of public/private keys in a second digital signature scheme; and the third party has a pair of public/private keys in a public key encryption scheme.

17. (New) The method according to claim 10, wherein the first party has a pair of public/private keys in a first digital signature scheme; the second party has a pair of public/private keys in a second digital signature scheme; and the third party has a pair of public/private keys in a public key encryption scheme.

18. (New) The method according to claim 11, wherein the first party has a pair of public/private keys in a first digital signature scheme; the second party has a pair of public/private keys in a second digital signature scheme; and the third party has a pair of public/private keys in a public key encryption scheme.